

1 Anna Hsia (SBN 234179)
2 ZWILLGEN LAW LLP
3 235 Montgomery Street, Suite 425
4 San Francisco, CA 94104
5 Telephone: (415) 590-2335
6 Facsimile: (415) 636-5965
7 anna@zwillgen.com

8 Attorneys for Defendant
9 **HYTTO LTD., D/B/A LOVENSE**

10 **UNITED STATES DISTRICT COURT**

11 **NORTHERN DISTRICT OF CALIFORNIA**

12 S.D.,

13 Plaintiff,

14 v.

15 HYTTO LTD., D/B/A LOVENSE,

16 Defendant.

Case No. 4:18-cv-00688-jsw

**SPECIALLY APPEARING DEFENDANT
HYTTO LTD., D/B/A LOVENSE'S REPLY
MEMO IN SUPPORT OF MOTION TO
DISMISS PLAINTIFF'S AMENDED
COMPLAINT FOR LACK OF PERSONAL
JURISDICTION AND FOR FAILURE TO
STATE A CLAIM**

Judge: Hon. Jeffrey S. White
Date: December 14, 2018
Time: 9:00 a.m.
Courtroom 5, 2nd Floor
1301 Clay Street
Oakland, CA 94612

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION 1

 I. Plaintiff Has Not and Cannot State a Claim Under the Wiretap Act or
 Common Law 1

 A. Hytto Did Not Intercept An “Electronic Communication” 2

 B. Operational Commands Are Not “Contents” Under the Wiretap
 Act..... 4

 C. Sending the Vibration Level of the Sex Toy is Not a Two-Party
 Communication..... 7

 D. The Alleged Interception Falls Within the Wiretap Act’s
 Ordinary Course of Business Exception..... 8

 E. Plaintiff’s Common Law Claims Should Be Dismissed..... 10

 II. The Court Lacks Personal Jurisdiction Over Hytto 12

 A. Plaintiff Cannot Establish Jurisdiction Based on Alleged
 Location of the Harm 12

 B. Offering an Interactive Website Accessible from the United
 States or Using a United States-Based Payment Provider Does
 Not Confer Jurisdiction..... 13

CONCLUSION..... 15

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Adobe Systems, Inc. v. Cardinal Camera & Video Ctr., Inc.</i> , 2015 WL 5834135 (N.D. Cal. Oct. 7, 2015).....	13, 14
<i>Axiom Foods, Inc. v. Acerchem Int’l Inc.</i> , 874 F.3d 1064 (9th Cir. 2017).....	13
<i>be2 LLC v. Ivanov</i> , 642 F.3d 555 (7th Cir. 2011).....	14
<i>Campbell v. Facebook Inc.</i> , 77 F. Supp. 3d 836 (N.D. Cal. 2014)	9, 10
<i>DEX Systems, Inc. v. Deutsche Post AG</i> , 727 Fed. Appx. 276 (9th Cir.)	15
<i>Francis v. API Technical Servs., LLC</i> , 2014 WL 11462449 (E.D. Tex. Sept. 11, 2014)	13
<i>Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.</i> , 905 F.3d 597 (9th Cir. 2018).....	12
<i>Gonzales v. Uber Technologies, Inc.</i> , 305 F. Supp. 3d 1078, 1080 (N.D. Cal.), <i>on reconsideration</i> , 2018 WL 3068248 (N.D. Cal. June 21, 2018)	5, 6
<i>Hall v. EarthLink Network Inc.</i> , 396 F.3d 500 (2d Cir. 2005).....	9
<i>Halperin v. Int’l Web Servs., LLC</i> , 70 F. Supp. 3d 893 (N.D. Ill. 2014)	4
<i>Helicopteros Nacionales de Colombia, S.A. v. Hall</i> , 466 U.S. 408 (1984)	14
<i>In re Facebook Internet Tracking Litig.</i> , 263 F. Supp. 3d 836 (N.D. Cal. 2017)	11
<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011)	8

1	<i>In re Google Inc. Gmail Litigation (“Gmail”),</i>	
2	2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)	9-10
3	<i>In re Google, Inc. Privacy Policy Litig.,</i>	
4	58 F. Supp. 3d 968 (N.D. Cal. 2014)	11
5	<i>In re Nickelodeon Consumer Privacy Litig.,</i>	
6	2014 WL 3012873 (D.N.J. July 2, 2014)	11
7	<i>In re Zynga Privacy Litig.,</i>	
8	750 F.3d 1098 (9th Cir. 2014).....	6
9	<i>Kirch v. Embarq Management Co.,</i>	
10	702 F.3d 1245 (10th Cir. 2012).....	9
11	<i>LiveCareer Ltd. v. Su Jia Technologies Ltd.,</i>	
12	2015 WL 1448505 (N.D. Cal Mar. 31, 2015)	15
13	<i>Low v. LinkedIn Corp.,</i>	
14	900 F. Supp. 2d 1010 (N.D. Cal. 2012)	11-12
15	<i>Mavrix Photo, Inc. v. Brand Technologies, Inc.,</i>	
16	647 F.3d 1218 (9th Cir. 2011).....	14
17	<i>Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.,</i>	
18	243 F. Supp. 2d 1073 (C.D. Cal. 2003).....	13
19	<i>Paccar International v. Commercial Bank of Kuwait, S.A.K.,</i>	
20	57 F.2d 1058 (9th Cir. 1985).....	12-13
21	<i>Pakootas v. Teck Cominco Metals Ltd.,</i>	
22	905 F.3d 565 (9th Cir. 2018).....	15
23	<i>Pebble Beach Co. v. Caddy,</i>	
24	453 F.3d 1151 (9th Cir. 2006)	13
25	<i>Professional’s Choice Sports Medicine Products, Inc. v. Hegeman,</i>	
26	2016 WL 1450704 (S.D. Cal. Apr. 12, 2016)	15
27	<i>Quokka Sports, Inc. v. Cup Int’l Ltd.,</i>	
28	99 F. Supp. 2d 1105 (N.D. Cal. 1999)	15
	<i>Rainsy v. Facebook, Inc.,</i>	
	311 F. Supp. 3d 1101 (N.D. Cal. 2018)	5
	<i>Rene v. G.F. Fishers, Inc.,</i>	
	817 F. Supp. 2d 1090 (S.D. Ind. 2011)	3, 4

1	<i>Taus v. Loftus</i> ,	
2	40 Cal. 4th 683 (2007)	10
3	<i>United States v. Reed</i> ,	
4	575 F.3d 900 (9th Cir. 2009).....	5
5	<i>United States v. Ropp</i> ,	
6	347 F. Supp. 2d 831 (C.D. Cal. 2004).....	3, 4
7	<i>United States v. Scarfo</i> ,	
8	180 F. Supp. 2d 572 (D.N.J. 2001)	4
9	<i>Walden v. Fiore</i> ,	
10	571 U.S. 277 (2014)	13
11	<i>White, et al. v Samsung Elec. Amer., Inc., et. al.</i> ,	
12	No. 17-1775 (D.N.J. Sept. 26, 2018)	8
13	<i>Yunker v. Pandora Media, Inc.</i> ,	
14	2013 WL 1282980 (N.D. Cal. Sept. 4, 2014)	5, 8

Statutes

15	18 U.S.C. § 2510(5)(a)	8-9
16	Fed. R. Civ. P. 4(k)(2)	12, 14

INTRODUCTION

An App provider’s collection of information about how people use that App is simply not an illegal wiretap, regardless of whether the App controls a thermostat or a sex toy. And when a device is used as a Bluetooth or infrared remote control for a local piece of hardware—be it a drone, a TV set, a sound speaker, or a sex toy—the communication is not the type of communication encompassed by the Wiretap Act. First, the communication is transmitted locally, and not in interstate commerce. Second, device commands are not the “contents of communications” under the Act. Third, even if the Act applied to such a transmission, capturing the operating data would be within several of the Act’s exceptions. For example, when a user directly inputs information into the App for the App to control the local device, either the App is the second party to the communication, or there is no second party to the communication. And where the purpose of the App is to control the volume or intensity level of the device, collecting those settings is within the Act’s ordinary course of business exception. Put simply, the Wiretap Act was never meant to apply here, and Plaintiff’s Opposition to Hytto’s Motion to Dismiss (the “Opposition”) provides no legal basis for an unprecedented extension of the well-established law.

The Amended Complaint (the “Complaint”) must also be dismissed because this court lacks personal jurisdiction over Hytto. Plaintiff does not dispute that Hong Kong-based Hytto has no physical presence in the United States and does not target advertisements specifically at the United States. Instead, she argues that it is good enough that she allegedly suffered injury in the United States, and points to a series of unremarkable aspects of Hytto’s website—that are common to most websites—as evidence that Hytto expressly aimed its actions at the United States. Neither Plaintiff’s alleged injury nor Hytto’s operation of an interactive website accessible from the United States confers personal jurisdiction over Hytto in every United States federal court.

I. Plaintiff Has Not and Cannot State a Claim Under the Wiretap Act or Common Law

Narrowing her Wiretap Act claim to cover only individuals who used the App with a partner does not save Plaintiff, as the Complaint still fails to allege the required elements of a Wiretap Act claim, and describes conduct expressly permitted by the Act. *First*, Plaintiff’s claim that interception of a purely local communication can violate the Act if that communication is

“internet-based” (i.e., originated from the Internet) conflicts with rulings by multiple courts that intercepting a local communication between a keyboard and a computer via a keylogger is *not* a Wiretap Act violation, even if what is typed eventually makes its way to the Internet. *Second*, the device settings Hytto allegedly intercepted are not content under the Wiretap Act—they are operational commands exempted from the Act’s coverage. *Third*, when an App user inputs information into an App, the App is a party to the communication or, if not, it is a one-party communication between the user’s phone and the toy. *Fourth*, where an App that Plaintiff claims is designed to control the volume or intensity of a paired sex toy collects that volume or intensity information, such collection falls squarely within the Act’s ordinary course of business exception. Plaintiff’s common law claims similarly fail.

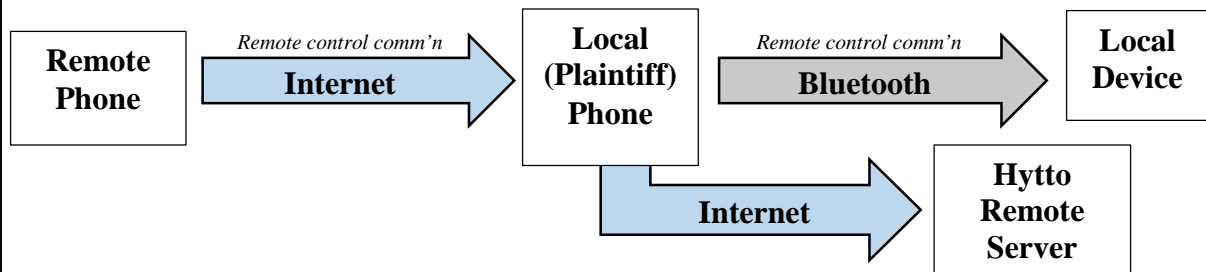
A. Hytto Did Not Intercept An “Electronic Communication”

Plaintiff has not alleged an actionable Wiretap Act claim because the interception is not alleged to occur while the transmission is travelling through a system that affects interstate commerce. Limiting the putative class to only those users that used the “Long Distance Control Feature” does not save Plaintiff’s Complaint. *See* Opp’n at 10. This is not a class issue, it is a definition of “electronic communication” issue. The alleged interception in this case occurs when the local user’s Body Chat app sends the operational commands to the toy via Bluetooth. *See, e.g.* FAC ¶ 29 (“Once downloaded, the Body Chat App allows users to ‘pair’ (i.e., connect) their Lovense devices to their smartphones using a Bluetooth connection. Through the Body Chat App, Defendant allows users to access and control their Lovense device’s full array of features and settings, including the various vibration intensities”); ¶ 35 (“Defendant fails to notify or warn customers that the Body Chat App monitors and records, in real time, how people use and communicate through these intimate devices and transmits the collected private information to its servers.”). Plaintiff nevertheless argues that the Act’s interstate commerce requirement is satisfied because the local communications between the toy and the App are “internet-based” in that they were previously sent from another user’s phone to the Plaintiff’s phone. This is wrong.

As explained in Hytto’s motion to dismiss, local communications cannot serve as a basis for Wiretap Act liability merely because the information collected previously or subsequently

travels in interstate commerce. Rather, the critical issue is *where* the interception allegedly occurred. *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090, 1094 (S.D. Ind. 2011) (no Wiretap Act claim because the alleged interception did not occur “while the transmission is traveling through a system that affects interstate or foreign commerce); *United States v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004) (no Wiretap Act claim for alleged interception of keyboard strokes, even when composing emails transmitted over the Internet).

Plaintiff’s attempts to distinguish *Rene*, *Ropp*, and similar cases fail. She argues that the keylogger software in those cases “doesn’t care if the computer is or is not connected to the internet.” Opp’n at 10, n.4. But that statement is true here too. The App does not care if the toy is being controlled by a person using their App and toy alone, or by the “remote” user. The alleged interception is the same. Plaintiff’s own diagram, re-pasted below, proves this point.



See Opp’n at 9. The communications at issue in this case are the ones exchanged between the “Local (Plaintiff) Phone” and the “Local Device” via Bluetooth. Both the communications that originate over the internet and the ones that the users type in are eventually sent locally between the “Local (Plaintiff) Phone” and the “Local Device.” If any type of “interception” occurs, it happens at the same point in transmission. Either both transmissions are covered or both are not covered. But Plaintiff concedes that the local communications are not covered. See *id.* The fact that the remote communications originally started elsewhere does not matter if the alleged interception takes place in the right-hand part of the diagram, which is what the Complaint alleges.

Plaintiff’s argument that the interstate commerce requirement is met because “this pathway *could not function* without an active internet connection” misses the mark. See *id.* It ignores the critical question of *where* the actual interception allegedly occurred. To state a claim, Plaintiff must allege that the interception occurred *while the communication traveled through a system that*

1 *affects interstate commerce*. The fact that interstate travel happened at some distant point is
 2 irrelevant, and such a novel theory would capture an inordinate number of activities in the Wiretap
 3 Act. For example, Plaintiff would find an “interception” where someone used a local video
 4 camera hidden on a bookshelf to record a Skype session on a computer, because the Skype call
 5 could not function without an internet connection. Under Plaintiff’s theory, the Wiretap Act
 6 likewise would apply to an intercept device placed on a speaker wire connecting an old-fashioned
 7 speaker to a regular stereo if the stereo were tuned to an Internet radio provider, but not if a local
 8 CD were playing. And recording a singing telegram with an old-fashioned tape recorder would
 9 violate the Wiretap Act so long as the telegram transmission originated out-of-state. These
 10 examples are not only absurd, but prior cases have reached directly the opposite conclusion,
 11 finding that “[t]he network connection is irrelevant to the transmissions, which could have been
 12 made on a stand-alone [iPhone] that had no link at all to the internet or any other external
 13 network.” *Ropp*, 347 F. Supp. 2d at 838; *see also United States v. Scarfo*, 180 F. Supp. 2d 572,
 14 581 (D.N.J. 2001) (finding that software that did not search for and record data entering or exiting
 15 the computer from the transmission pathway through the modem attached to the computer did not
 16 violate Wiretap Act).

17 Plaintiff’s claim cannot proceed merely because she purports to limit her class to
 18 transmissions that originated from the Internet. The court in *Rene* did not find that plaintiff’s
 19 Wiretap Act claim could proceed where she was typing on the Internet (such as “accessing her
 20 email and personal checking accounts”) but not where she was typing locally in Microsoft Word.
 21 *See Rene*, 817 F. Supp. 2d at 1092; *see also Halperin v. Int’l Web Servs., LLC*, 70 F. Supp. 3d
 22 893, 902 (N.D. Ill. 2014) (rejecting Wiretap Act claim where software captured a “transmission
 23 that require[s] no connection to the outside world,” even though the information allegedly
 24 captured originated from the world wide web) (internal quotation marks and citation omitted).

25 **B. Operational Commands Are Not “Contents” Under the Wiretap Act**

26 The conduct alleged in this case also cannot violate the Wiretap Act because the
 27 information Hytto allegedly intercepted does not constitute the “contents” of communications
 28 under the Wiretap Act. The information allegedly “intercepted” by the App is the date and time of

1 each use and the vibration intensity level of the device. *See* FAC ¶ 36. The Opposition does not
2 argue that the date and time of use are contents under the Act. Indeed, it is well settled that such
3 information is **not** content. *See, e.g. United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009)
4 (holding that information about a telephone call’s origination, length, and time was not content).
5 The Opposition hangs its hat on the vibration intensity level of the device being content. It is not.

6 The Wiretap Act has never been interpreted to cover operational commands like “raise the
7 volume one notch,” “turn off the lights,” or “increase the vibration intensity level” of a sex toy. If
8 it were, every time a phone was used as a remote control, it would violate the Wiretap Act if the
9 app stored a record of that command. Plaintiff points to no cases dictating such a result. Indeed,
10 none of Plaintiff’s cases involve operational commands. *Rainsy v. Facebook, Inc.*, involved
11 “liking” a Facebook page, which the court said was content because it “communicates approval”
12 of the page. 311 F. Supp. 3d 1101, 1114-15 (N.D. Cal. 2018). *Yunker v. Pandora Media, Inc.*,
13 involved the communication of personally identifiable information. 2013 WL 1282980, at *7
14 (N.D. Cal. Sept. 4, 2014). And *Gonzales v. Uber Technologies, Inc.* involved the price and geo-
15 location of ride-sharing. 305 F. Supp. 3d 1078, 1080 (N.D. Cal.), *on reconsideration*, 2018 WL
16 3068248 (N.D. Cal. June 21, 2018).

17 The Opposition tries to get great mileage out of the fact that this case involves a sex toy,
18 repeatedly describing the vibration intensity as “intimate communications” or “incredibly intimate
19 information” that it is “creepy” for the App to collect (even though users input it into the App).
20 But a simpler way to see the misguided nature of Plaintiff’s theory is to consider if the app were
21 being used to control another in-home device. For example, if it were an app that allowed a
22 homeowner to connect to their thermostat to set the temperature, no one would consider the degree
23 setting on the thermostat to be within the scope of the Wiretap Act. Plaintiff tries to get around
24 this limitation on the Wiretap Act’s scope by re-characterizing the operational command as a
25 statement by the person providing the command that “I want to cause your sex toy to vibrate at
26 this intensity level.” Opp’n at 12. This attempt to shoehorn non-content into content fails because
27 the same technique could be used for any device setting. For example, using an app to raise the
28 volume on a television could be a statement that “I want to cause the TV to play at this volume.”

1 Using an app to turn off lights could be a statement that “I want to sit in the dark.” But courts do
 2 not accept this approach. For example, header information—the portion of a webpage that
 3 provides the address of the webpage from which the request was sent—has been held to not be
 4 content under the Wiretap Act. *See, e.g., In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106-7 (9th
 5 Cir. 2014). It is not viewed as a statement that the user “wants to visit the webpage.”

6 Plaintiffs own cases reject such a malleable interpretation of content. In *Gonzales*, plaintiff
 7 argued that a Lyft driver’s toggling on the Lyft App constitutes content because it conveys the
 8 message that “the driver is available [or, in Plaintiff’s parlance, “wants to”] work. *Gonzales*, 305
 9 F. Supp. 3d at 1085-86. The court conceded that was one possible inference that could be drawn,
 10 but noted that another was that the driver hit the switch for whether he wants to work or not. *Id.*
 11 The court then found that the only communication then, was that the driver turned on the app—“a
 12 communication more akin to record information than content.” *Id.* at 1086. Citing *Zynga*, the
 13 court reasoned:

14 Under Plaintiff’s interpretation of “content,” the information as to the webpage the user
 15 was viewing is content because it can be inferred that the user was communicating he
 16 wanted to view that webpage, just as, according to Plaintiff, from the act of toggling on it
 17 can be inferred that driver is available to accept rides. But *In re Zynga* rejects such a broad
 reading of content. In other words, simply opening a webpage or mobile application is not
 a communication with content.

18 *Id.* So too here. Simply opening an app and setting the volume or intensity of a sex toy (or radio
 19 or television) is not a communication with content.

20 Plaintiff concedes that Hytto “may have a point” that vibration intensity is not content
 21 where a user is using the App and toy alone, but suggests that the result should be different where
 22 users are using the App and toy with a partner. *See Opp’n* at 12. But she does not explain why
 23 the nature of vibration intensity would be different merely because it is being transmitted between
 24 two persons as opposed to a person and a server like in *In re Zynga* and *Gonzales*. Nor does she
 25 point to any cases stating that such a distinction matters for purposes of determining whether
 26 something is content under the Wiretap Act. The distinction Plaintiff seeks to draw also makes
 27 little sense. Would the record of a thermostat temperature change be non-content if a local user
 28

1 uses her app to change the temperature, but become content if the app maker introduces a feature
 2 that allows a remote user to change the temperature using their app while someone else is in the
 3 house? In both cases the information—the temperature setting—would be the same and would not
 4 be content under existing caselaw.

5
 6 **C. Sending the Vibration Level of the Sex Toy is Not a Two-Party Communication**

7 Plaintiff’s Wiretap Act claim must also be dismissed because the communication at issue is
 8 either a one-party communication between an App user and the toy, or a communication to which
 9 Hytto is a party. Neither scenario can present a Wiretap Act violation.

10 The Opposition responds to the argument that Hytto is a party to the communication by
 11 calling such a notion “creepy.” *See* Opp’n at 12. But the Opposition ignores the argument that
 12 these are all one-party communications between the user and the sex toy. If Hytto is not a party to
 13 the communication, there is no second party to the communication. If an individual were using
 14 the App and toy alone, that individual would enter the desired vibration level into the App and it
 15 would be transmitted to the toy. The Opposition does not dispute that such a communication
 16 would be a one-party communication between the user and his or her toy—not subject to Wiretap
 17 Act protection. Plaintiff alleges that when the “Long Distance Control” function is in use, a
 18 remote partner is controlling the vibration intensity of the toy. *See* FAC ¶ 30. But that remains a
 19 one-party communication, just with a different person as the party. If a remote user changes the
 20 volume of the home stereo it does not become a two-party communication just because someone is
 21 at home inside the house listening to music. Here, whichever party is controlling the sex toy
 22 would be the only party to the communication other than perhaps Hytto.

23 The Opposition’s conclusory statement that the communications at issue are between
 24 Plaintiff and her partner are contradicted by the Complaint itself. *See* Opp’n at 13. That is simply
 25 not how the Complaint describes the long distance control feature operating. *See* FAC ¶ 44
 26 (noting that Plaintiff used the “Long Distance Control” feature, “wherein her device would be
 27 controlled remotely by a third party...”); *see also id.* at ¶¶ 1, 32, 35. Nor is it what is shown in the
 28 diagram in Plaintiff’s Opposition, in which the Plaintiff’s local phone is claimed to be a “pass-

1 through.” *See* Opp’n at 9. That is just a less direct way of saying her partner’s device was
 2 controlling the toy—which would be a one party communication between her partner and the toy.

3 If there is any second party to the relevant communication here, it is Hytto. Numerous
 4 courts have found that when a user enters data into an app, browser, or similar platform, the
 5 provider is the second party to the communication. For example, in *Yunker*, this Court found that
 6 there was no actionable Wiretap Act claim where plaintiff alleged that Pandora “intercepted”
 7 personally identifiable information that Plaintiff “expressly alleges that he communicated [] to
 8 Pandora” because Pandora would have been a party to such communication. 2013 WL 1282980,
 9 at *8. Similarly, in *In re Facebook Privacy Litig.*, the court found that a plaintiff clicking on an
 10 advertisement banner on Facebook’s website would constitute a communication sent from the user
 11 to Facebook, subject to the Wiretap Act’s party to the communication exception. 791 F. Supp. 2d
 12 705, 713 (N.D. Cal. 2011). More recently, a New Jersey District Court found that the exception
 13 applied to information users input into Smart TVs. *See* Letter Order, *White, et al. v Samsung Elec.*
 14 *Amer., Inc., et. al.*, No. 17-1775 (D.N.J. Sept. 26, 2018) (attached as Exhibit A to Declaration of
 15 Ann Hsia). There, plaintiffs alleged that defendants violated the Wiretap Act because their
 16 internet connected Smart TVs captured users’ viewing selections. Defendants moved to dismiss,
 17 arguing that “[w]hether Plaintiffs’ intended focus is on the communications that Defendants’
 18 Smart TVs transmit to Plaintiffs at Plaintiffs’ own requests or those sent to Defendants’ servers . .
 19 . Defendants are direct participants in all relevant communications.” *Id.* at 6. The court agreed
 20 and dismissed plaintiffs’ Wiretap Act claim. The same can be said here: if there is a second party
 21 to the communication, because the relevant communication is with the Body Chat App, Hytto is
 22 that second party.

23 **D. The Alleged Interception Falls Within the Wiretap Act’s Ordinary Course**
 24 **of Business Exception**

25 Under the Wiretap Act’s ordinary course of business exception, “[a]ny telephone or
 26 telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider
 27 of wire or electronic communication service in the ordinary course of its business” is not an
 28 electronic, mechanical, or other device, and thus does not fall under the definition of “intercept”

1 under the Act. *See* 18 U.S.C. § 2510(5)(a). As another court in this district recently held, an
2 interception falling within the exception “must be related or connected to an electronic
3 communication provider’s service, even if it does not actually facilitate that service.” *Campbell v.*
4 *Facebook Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014). The collection Plaintiff alleges meets
5 this description.

6 Plaintiff alleges that the service the App provides is to control the volume or intensity of
7 the paired sex toy. *See* FAC ¶¶ 29, 35. Common sense dictates that the App’s collection of
8 volume or intensity settings is related or connected to that service. Decisions by other courts
9 support this conclusion. For example, in *Hall v. EarthLink Network Inc.*, the Second Circuit found
10 the exception satisfied where email provider EarthLink was alleged to have continued to receive
11 emails after users terminated their accounts because receiving emails was within EarthLink’s
12 ordinary course of business. 396 F.3d 500, 505 (2d Cir. 2005). Similarly, in *Kirch v. Embarq*
13 *Management Co.*, the Tenth Circuit found the exception satisfied where an ISP was alleged to
14 have intercepted electronic communications over its network because the ISP had access to “no
15 more of its users’ electronic communications than it had in the ordinary course of its business as
16 an ISP.” 702 F.3d 1245, 1250 (10th Cir. 2012). So too here. Transmitting volume or intensity
17 settings is the App’s alleged purpose, and Hytto had no more access to users’ communications
18 than it had in its business as a provider of the App that controls the volume or intensity settings.

19 The Opposition urges the Court to adopt the narrower standard articulated in *In re Google*
20 *Inc. Gmail Litigation* (“Gmail”), 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)—which states that
21 in order to satisfy the exception the alleged interception must “facilitate[] the transmission of the
22 communication at issue or [be] incidental to the transmission of such communication.” *See* Opp’n
23 at 13-14. As an initial matter, *Gmail* is an outlier. Even other courts within this district have
24 declined to follow its narrow interpretation of the ordinary course exception. *See Campbell*, 77 F.
25 Supp. 3d at 844. Hytto’s conduct nonetheless satisfies even *Gmail*’s narrower standard. The
26 Complaint repeatedly characterizes the ability to control the toy’s volume or intensity level as the
27 fundamental purpose of the App. Hytto collects volume or intensity level as part and parcel of that
28 ability. At the very least Hytto’s collection is “incidental” to that service, if not “facilitating” it.

1 Plaintiff does not allege that Hytto collects vibration or intensity level for any purpose other than
 2 delivery of the service. This differs from *Gmail* where Plaintiff alleged that Google was scanning
 3 the content of users emails in order to facilitate its delivery of targeted advertising, and to create
 4 user profiles to serve their profit interests *that were unrelated* to providing email services to
 5 particular users. *See Gmail*, 2013 WL 5423918, at *11. There is no similar allegation here.

6 Plaintiff's argument that the exception should not apply because she alleges the
 7 interceptions were contrary to Hytto's stated practices must also be rejected. *See Opp'n* at 14. For
 8 one, Plaintiff misrepresents Hytto's stated practices.¹ But even if that were not the case, the only
 9 case Plaintiff cites in support of her argument is *Gmail*. But as another court in this district held,
 10 *Gmail's* finding that Google violated its own internal policies "was not critical to the court's
 11 rejection of the 'ordinary course of business' exception." *Campbell*, 77 F. Supp. 3d at 845. The
 12 *Gmail* court had already found that Google's interceptions were "neither instrumental to the
 13 provision of email services, nor are they an incidental effect of providing these services." *Id.*
 14 Here, as Plaintiff concedes, the App's collection of vibration intensity as it is being used to control
 15 the intensity of the toy is instrumental to the services the App provides or, at the very least an
 16 incidental effect of providing those services. The ordinary course of business exception thus
 17 applies.

18 **E. Plaintiff's Common Law Claims Should Be Dismissed**

19 Plaintiff's intrusion upon seclusion and unjust enrichment claims also cannot survive.
 20 Intrusion upon seclusion requires an intrusion that is highly offensive to a reasonable person.
 21 *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007). Hytto's collection of information provided to it by
 22 users of the App cannot be highly offensive to a reasonable person. Both the Electronic
 23 Communications Privacy Act and the Wiretap Act allow providers of a communication system to
 24 access communications. Thus, email providers can "see" highly personal emails, even ones that

25
 26 ¹ Specifically, Plaintiff alleges that the App's collection of Usage Information runs contrary to
 27 Hytto's statement in its FAQs that "All data transfers are peer-to-peer." *See* FAC ¶ 33. But that
 28 statement relates to the previous sentence stating that "Absolutely no sensitive data (pictures,
 video, chat logs) pass through (or are held) on our servers." *Id.* It says nothing about the
 collection (or non-collection) of operational commands.

1 might be about sex acts, and Google can “see” browsing histories, which could include sexual
2 content, without it constituting an intrusion upon seclusion. *See, e.g., In re Google, Inc. Privacy*
3 *Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (finding that Google’s collection of
4 browsing histories does not rise to the necessary level of intrusion).

5 In the same way, Hytto has access to the vibration intensity settings the users directly input
6 into the App. A person who does not want the vibration intensity setting of a sex toy exposed to
7 the sex toy company (not the world), can choose not to provide the data to the sex toy company; or
8 not buy a toy that is remotely controlled through an App provided by the sex toy company. But if
9 the user chooses to provide the data to the App, no reasonable person would find the App’s
10 collection of such information “highly offensive.” This holds true whether users provide
11 information to a sex toy app or the Angry Birds app. *See* Opp’n at 15. In either case, such matters
12 of routine Internet functionality are not highly offensive. *See In re Facebook Internet Tracking*
13 *Litig.*, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017) (“Since these requests are part of routine internet
14 functionality and can be easily blocked, the Court finds that they are not a ‘highly offensive’
15 invasion of Plaintiffs’ privacy interests.”); *see also In re Nickelodeon Consumer Privacy Litig.*,
16 2014 WL 3012873, at *19 (D.N.J. July 2, 2014) (dismissing invasion-of-privacy claim because
17 plaintiffs failed to show that defendants’ “collection and monetization of online information,”
18 including users’ browsing histories, “would be offensive to the reasonable person, let alone
19 exceedingly so”).

20 Plaintiff’s unjust enrichment claim also should be dismissed. To cure the Complaint’s
21 failure to identify a specific state law in her unjust enrichment claim, Plaintiff uses her Opposition
22 to allege applicability of Georgia law. *See* Opp’n at 15. But because the elements for unjust
23 enrichment under Georgia law are similar to those under California law, Plaintiff’s unjust
24 enrichment claim still fails for the reasons identified in Hytto’s initial brief. *See* Def.’s
25 Memorandum of Points and Authorities (Dkt. 36) (“Mem.”) at 15. Moreover, Plaintiff should not
26 be allowed to re-plead where she has already amended once and was on notice of this pleading
27 failure prior to that amendment (because Hytto raised it in its motion to dismiss the original
28 complaint). *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) (courts may deny

a plaintiff leave to amend if the plaintiff had opportunities to amend its complaint and failed to cure deficiencies).

II. The Court Lacks Personal Jurisdiction Over Hytto

The Complaint also fails because even after conducting jurisdictional discovery, Plaintiff cannot establish specific jurisdiction over Hytto under Federal Rule 4(k)(2). Plaintiff does not dispute that China-based Hytto has no employees, offices, or real estate in the United States; does not pay taxes in the United States; and does not target print, radio, direct mail, or Internet advertisements specifically at the United States or its citizens. Declaration of Chris Dabreo (Dkt. 36-1) (“Dabreo Decl.”) ¶¶ 6-9. Nor does she identify any meaningful Hytto actions that are expressly aimed at the United States as opposed to any jurisdiction the Internet reaches. Instead, Plaintiff first tries to cherry-pick language from inapplicable cases to create a new test for specific jurisdiction, and then points to a series of irrelevant aspects of Hytto’s website. Both efforts fail.

A. Plaintiff Cannot Establish Jurisdiction Based on Alleged Location of the Harm

Plaintiff first attempts to avoid the well-settled requirement under Rule 4(k)(2) that a defendant must have purposefully directed its actions at the United States. She emphasizes that under “recent” Ninth Circuit law, it is enough that Hytto commit an intentional tort that harmed United States residents. Opp’n at 4. The argument relies on a misreading of *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Group*, 905 F.3d 597 (9th Cir. 2018). The Ninth Circuit in that case found purposeful direction to support jurisdiction because defendant made the alleged defamatory statement while physically present in the forum state. *Id.* at 607 (“[I]n the instant case, [defendant] voluntarily traveled to Nevada to attend the aviation industry conference, and voluntarily agreed to speak with Shvetsova and Khalek there.”). Indeed, *Freestream* expressly distinguished situations, like here, where a defendant was not physically present in the forum state. *Id.* at 605 (“Importantly, unlike the case at hand, neither *Yahoo!* nor *Mavrix* involved an alleged tort committed while defendant was physically present in the forum state.”).²

² Plaintiff’s other cases are similarly distinguishable. In *Paccar International v. Commercial Bank of Kuwait, S.A.K.*, the court found that defendant’s fraudulent demand for payment made directly to a California bank was enough to constitute express aiming. 757 F.2d 1058, 1064 (9th

Rule 4(k)(2) requires that defendant purposefully directed its actions at the United States. *See Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1159 (9th Cir. 2006); *see also Walden v. Fiore*, 571 U.S. 277, 290 (2014) (“The proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant’s conduct connects him to the forum in a meaningful way.”); *see also Axiom Foods, Inc. v. Acerchem Int’l Inc.*, 874 F.3d 1064, 1068 (9th Cir. 2017) (noting that “the minimum contacts analysis examines the defendant’s contacts with the forum State itself, not the defendant’s contacts with persons who reside there”) (internal quotation marks and citation omitted); *Adobe Sys., Inc. v. Cardinal Camera & Video Ctr., Inc.*, 2015 WL 5834135, at *5 (N.D. Cal. Oct. 7, 2015) (“Random, fortuitous, or attenuated contacts with individuals in the forum are insufficient to support personal jurisdiction.”) (internal quotation marks and citation omitted). Plaintiff fails to establish such purposeful direction.

B. Offering an Interactive Website Accessible from the United States or Using a United States-Based Payment Provider Does Not Confer Jurisdiction

Plaintiff next contends that Hytto’s operation of an interactive website accessible in the United States establishes express aiming. This argument fails. Random contacts with a forum that are unrelated to the underlying claim do not support jurisdiction. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 243 F. Supp. 2d 1073, 1085 (C.D. Cal. 2003) (“contacts may only be considered for purposes of the jurisdictional analysis if they are sufficiently related to the underlying causes of action.”). Here, Plaintiff identifies a number of contacts irrelevant to her claim that Hytto “intercepts” the Bluetooth transmission of usage information between the App and her toy. FAC ¶ 37. For example, Hytto offering an affiliate program with advertisements in English and commissions calculated in U.S. dollars (Opp’n at 6-7) is irrelevant to Plaintiff’s Wiretap Act claim, regardless of Plaintiff’s participation in such program. *See* FAC ¶¶ 40-49. Nor does the existence of

Cir. 1985). Similarly, the out-of-forum case Plaintiff cites involved an individual defendant that hacked into the home IP address of an individual plaintiff that defendant knew lived in Texas. *See Francis v. API Tech. Servs., LLC*, 2014 WL 11462449, at *4 (E.D. Tex. Sept. 11, 2014) (“[I]t is reasonable for [defendant] to expect to be haled into a Texas court because he, or someone acting at his direction, allegedly intentionally obtained access to [plaintiff’s] personal G-Mail accounts, blocked [plaintiff’s] from obtaining access to these accounts, improperly used [plaintiff] and his family’s personal information and hacked into plaintiff’s home IP address.”).

1 testimonials from U.S. customers on Lovense.com establish express aiming (*see* Opp’n at 6), since
 2 “unilateral activity of another party or a third person is not an appropriate consideration when
 3 determining whether a defendant has sufficient contacts with a forum State to justify an assertion of
 4 jurisdiction.” *Helicopteros Nacionales de Colom., S.A. v. Hall*, 466 U.S. 408, 417 (1984).

5 Plaintiff also cannot establish jurisdiction by virtue of Hytto offering a website accessible to
 6 U.S. residents. She identifies a series of “actions”—Hytto’s website displays text in English;
 7 includes ads from U.S. businesses; has traffic from U.S. users; lists the U.S. first in the country drop
 8 down menu—but such characteristics apply to nearly any website accessible from the United States.
 9 These unremarkable characteristics do not constitute express aiming, even when taken together. *See*
 10 *be2 LLC v. Ivanov*, 642 F.3d 555, 559 (7th Cir. 2011) (“If the defendant merely operates a website,
 11 even a ‘highly interactive’ website, that is accessible from, but does not target, the forum state, then
 12 the defendant may not be haled into court in that state without offending the Constitution.”).
 13 Likewise, the mere sale of products into the United States does not support jurisdiction. *See* Mem. at
 14 7. Plaintiff does not allege in any non-conclusory way that Hytto targets advertisements to the U.S.,
 15 markets products specifically intended for a U.S. audience, or in any other way directs its sales
 16 activities to the U.S. as opposed to elsewhere. *Adobe Sys. Inc.*, 2015 WL 5834135, at *5.

17 Plaintiff cites to *Mavrix Photo, Inc. v. Brand Technologies, Inc.*, 647 F.3d 1218 (9th Cir.
 18 2011) as supporting a finding of jurisdiction where website traffic includes a substantial number of
 19 U.S. residents. But if that were enough to establish personal jurisdiction anyone could manufacture
 20 jurisdiction by bombarding a defendant’s website, regardless of whether defendant expressly aimed
 21 its website at that jurisdiction. That is not the law. Indeed, the *Mavrix* plaintiff established
 22 jurisdiction by showing that the website displayed third-party advertisements aimed at California
 23 residents, which demonstrated that defendant knew about its California user base “and that it
 24 exploits that base for commercial gain by selling space on its website for advertisements.” *Id.* at
 25 1230. There is no similar allegation of advertising targeted at U.S. residents here. Rather, it is
 26 undisputed that Hytto does not target Internet advertisements specifically at the United States or
 27 United States citizens. Dabreo Decl. ¶ 9.

28 Plaintiff’s other cases (*see* Opp’n at 6-7) are similarly mischaracterized or otherwise

distinguishable from the case at hand. For example, Plaintiff contends *Professional's Choice Sports Medicine Products, Inc. v. Hegeman*, 2016 WL 1450704, at * 5 (S.D. Cal. Apr. 12, 2016) shows that Hytto's use of PayPal "demonstrates a high level of interactivity." Opp'n at 6. But Plaintiff omits the rest of the quote explaining that such interactivity is *insufficient* to confer jurisdiction. See *Prof's Choice*, 2016 WL 1450704, at *5 (noting that the case "cited by Plaintiff to the contrary, merely holds that the use of PayPal demonstrates a high level of interactivity for the web-site, not that the use of a California-based third-party payor conveys jurisdiction on California."). Indeed, the court expressly held that "[a]llowing California to have jurisdiction over every internet business that uses PayPal would be a clear violation of due process." *Id.* It would be even more of a due process violation to allow any court in the United States to have jurisdiction over an internet business because it uses PayPal.³

CONCLUSION

For the foregoing reasons, and those stated in Hytto's original memorandum, this Court should dismiss the Amended Complaint with prejudice.

DATED: November 1, 2018

ZWILLGEN LAW LLP

By: /s/ Anna Hsia

Anna Hsia (SBN 234179)

anna@zwillgen.com

Jeffrey Landis (admitted *Pro Hac Vice*)

jeff@zwillgen.com

Attorneys for Defendant

Hytto Ltd., d/b/a Lovense

³ See also *Quokka Sports, Inc. v. Cup Int'l Ltd.*, 99 F.Supp.2d 1105, 1112 (N.D. Cal. 1999) ("Defendants admitted that they sought out a specific domain to target the 'lucrative American market.'"); *Pakootas v. Teck Cominco Metals Ltd.*, 905 F.3d 565, 578 (9th Cir. 2018) ("inconceivable that [defendant] did not know its waste was aimed at the State of Washington when [it] deposited waste into the powerful Columbia river just miles upstream of the border."); *DEX Systems, Inc. v. Deutsche Post AG*, 727 Fed. Appx. 276, 278 (9th Cir.) (allegedly infringing use of plaintiff's software occurred on servers in California) (*petition for cert. filed*, No. 18-165 (Aug. 3, 2018); *LiveCareer Ltd. v. Su Jia Techs. Ltd.*, 2015 WL 1448505 (N.D. Cal. Mar. 31, 2015) (one of defendant's minority partners managed defendant's advertising campaigns with Google and Bing from an office located in California).